REMARKS

Claims 1-37 remain in the application with claims 1, 2, 14, 15 and 27 having been amended hereby. Claims 1, 14 and 27 are in independent form.

Reconsideration is respectfully requested of the rejection of claims 1-37 under 35 U.S.C. 103(a) as being unpatentable over Burns et al. (US 5,831,947) in view of Cooper (US 5,737,516).

An object of the present invention is to offer a secured contents transfer. In the independent claims, as amended, the first identification data, for example a machine ID, is sent from a terminal equipment with contents that are enciphered by the second identification data, for example a machine key, by referring to the identification database at a server apparatus. Each terminal equipment has its own first identification data and corresponding second identification data. Because there are many items of terminal equipment, the identification database indicates the relationship between a plurality of first identification data and a plurality of second identification data. The first identification data (machine ID) is transferred from the terminal equipment to the server apparatus. Therefore the first identification data (machine ID) is disclosed to the outside so it may be stolen during the transfusing process. Even if the first identification data (machine ID) is stolen, the

enciphered contents can not be restored because the contents are enciphered using the second identification data (machine key) corresponding to the first identification data (machine ID) at the server apparatus by referring the transferred first identification data (machine ID) from the terminal equipment.

In Burns et al., the access key can be made using the user ID (subscriber list), object ID, and owner key. The Examiner contents that Burns et al. col. 6, lines 38-39, is equivalent to the encryption unit for encrypting data to be sent over an insecure network wherein the data enciphered is based on the second identifier. The cited portion of Burns et al. holds that "such a request specifies an object id, an entry tag, and a lookup key." But Burns et al. neither teaches nor suggests that the data is encrypted based on the second identification data read out from the identification database corresponding to the first identification data transmitted from the first transmitting/receiving unit.

The cited references neither teach nor suggest that an identification database indicates the relationship between a plurality of first identification data and a plurality of second identification data. In the present invention, the terminal equipment transmits the first identification data, however, the data is encrypted based on the second identification data based

on the identification database by referring the transmitted first identification data. The second identification data which is used to encrypt the data is never disclosed to the outside during the transferring process because it is not transferred at all between the terminal equipment and the server apparatus (the terminal equipment and the server apparatus includes the second identification data from the first time). Even if the first identification data is stolen during the transferring process, the data may not be decrypted because no information about the second identification data can be gained from the stolen first identification data.

Moreover, the Examiner contends that the machine ID described in Cooper is equivalent to the first identification data of the present invention. However, Cooper uses the machine ID directly for encrypting and decrypting (see Figs. 4 and 20). The machine ID is transferred from a customer to a vendor (see Fig. 5), so it could be stolen during the transferring process. Once the machine ID is stolen, the person having the machine ID can restore the encrypted data because the machine ID can be directly used for the decryption process (see Fig. 20).

Therefore, the cited references neither teach nor suggest that data is encrypted based on the second identification data read out from the identification database corresponding to the

first identification data transmitted from the first transmitting/receiving unit. In the present invention, the user does not send/receive any encryption/decryption key from the server apparatus (from the very first time, the terminal equipment has its own encryption/decryption key corresponding to the terminal equipment by referring the transferred first identification data) also, information directly used to encrypt the data is not transferred between the terminal equipment and the server apparatus.

Therefore, the present invention can transfer data more securely than the processes of the cited art.

Therefore, by reason of the amendments made to the claims hereby, as well as the above remarks, it is respectfully submitted that data distributing apparatus and terminal apparatus for data distribution, as taught by the present invention and as recited in the amended claims, is neither shown nor suggested in the cited references.

The references cited as of interest have been reviewed and are not seen to show or suggest the present invention as recited in the amended claims.

Entry of this amendment is earnestly solicited, and it is respectfully submitted that the amendments made to the claims hereby raise no new issues requiring further consideration and/or search, because all of the features of this invention have

clearly been considered by the examiner in the prosecution of this application and because the present amendments serve only to further define and emphasize the novel features of this invention.

Favorable reconsideration is earnestly solicited.

Respectfully submitted,

COOPER & DUNHAM LLP

Jay H. Maioli
Reg. No. 27, 213

JHM/JBG